Ekaia, 2021, 41, 311-320
https://doi.org/10.1387/ekaia.22955

ekaia
ZIENTZIA eta TEKNOLOGIA ALDIZKARIA

ISSN 0214-9001 – eISSN 2444-3255

Talde abeldar finituetarako Galoisen alderantzizko problema

(The inverse Galois problem for finite abelian groups)

Maialen Gago Fruniz, Leire Legarreta Solaguren*

Matematika Saila, Zientzia eta Teknologia Fakultatea (UPV/EHU)

LABURPENA: Galoisen alderantzizko problema honetan datza: talde (finitu) bat emanda, Galoisen hedadura bat ea existitzen den zehaztea, zeinentzat hedadura horri dagokion Galoisen taldea hasieran emandako taldearen isomorfoa baita. Artikulu honen helburua izango da Kronecker-Weberren teorema frogatzea, edo, bestera esanda, edozein talde abeldar finitu $\mathbb{Q}$-ren gaineko Galoisen hedadura baten Galoisen taldearen isomorfoa dela frogatzea. Artikulu honetan, froga horri eusteko beharrezkoak diren hainbat kontzeptu eta emaitzen pintzelkadak aipatuko eta aurkeztuko dira: hasteko, aljebraren oinarrizko zenbait emaitza, polinomioei eta kongruentziei dagozkionak, azalduko dira; gero, Galoisen teoriaren oinarrizko definizio eta teoremak eta hedadura ziklotomikoen inguruko apunte batzuk aurkeztuko dira; eta, azkenik, Kronecker-Weberren teorema enuntziatu eta frogatuko da, aurretik azaldutako emaitza guztiak aintzat harturik.

HITZ GAKOAK: taldea, gorputza, hedadura, isomorfismoa, automorfismoa, ziklotomikoa, Galois, Galoisen alderantzizko problema, Kronecker-Weberren teorema.

ABSTRACT: *The inverse Galois problem wonders about the question whether any given finite group is isomorphic to the Galois group of a Galois extension. In this article, we will prove the Kronecker-Weber theorem, or in other words, that any abelian finite group is isomorphic to the Galois group of a Galois extension over $\mathbb{Q}$. In this article, a number of concepts and brushstrokes of the necessary results to support this proof will be mentioned and presented: first, certain fundamental results of algebra, corresponding to polynomials and congruences; then, the fundamental definitions and theorems of Galois theory, and some notes of cyclotomic extensions; and finally, Kronecker-Weber theorem will be enunciated and proved, taking into account all the previous results.*

KEYWORDS: group, field, extension, isomorphism, automorphism, cyclotomic, Galois, inverse Galois problem, Kronecker-Weber theorem.

**** Harremanetan jartzeko / Corresponding author:*** Maialen Gago Fruniz. Matematika Saila, Zientzia eta Teknologia Fakultatea (UPV/EHU), Sarriena auzoa (48940 Leioa, Bizkaia). – maialen.gago@gmail.com – https://orcid.org/

Nola aipatu / How to cite: Gago Fruniz, Maialen; Legarreta Solaguren, Leire (2021). «Talde abeldar finituetarako Galoisen alderantzizko problema». *Ekaia*, 41, 2021, 311-320. (https://doi.org/10.1387/ekaia.22955).

Jasotze-data: 2021, ekainak 30; Onartze-data: 2021, uztailak 26.

ISSN 0214-9753 - eISSN 2444-3581 / © 2021 UPV/EHU

1. SARRERA

Évariste Galois XIX. mendearen hasieran jaiotako matematikari frantsesa izan zen. Aurkikuntza iraultzaileak egin zituen arren, edo agian arrazoi beragatik, lortutako emaitzekin argitaratu nahi izan zituen memoria guztiak baztertu zizkioten garaiko matematikari esanguratsuenek. Bera izan zen, besteak beste, *talde* terminoa matematikaren testuinguruan erabili zuen lehena. 20 urte zituela hil zuten tiroz, eta bere lanek gerora *Galoisen teoria* izenez ezagutzen den teoria oso bat garatzeko argudioak utzi zituzten. (Ikusi [1].)

Galoisen teoria Aljebra abstraktuaren adar nagusietako bat da, eta teoria horrek gorputzen teoriaren eta talde-teoriaren arteko lotura erakusten du. F/K erako Galoisen hedadurek sortzen dituzten Galoisen taldeak azter daitezke, eta eztabaidatu daiteke ea talde horiek ezagunak ditugun talde mota batzuen isomorfoak diren ala ez.

Beharbada, ikerketa-munduan ez da Galoisen alderantzizko probleman horrenbeste sakondu. Galoisen alderantzizko problema, zehazki, honetan datza: G taldea (finitua) emanda, F/K erako Galoisen hedadura existitzen den zehaztea, non $G \cong \mathrm{Gal}_K(F)$ baita. Halako kasuetan, G taldea Galoisen hedadura gisa gauzatu daiteekela, edo, laburrago, G taldea gauzatu daitekeela esango dugu.

Problema horrek, oraindik ere, hainbat kasutarako erantzunik ez duen arren, artikulu honetan talde abeldar finituak $\mathbb{Q}$-ren gaineko Galoisen talde gisa gauzatu daitezkeela aztertuko dugu; Kroneckerrek eta Weberrek XIX. mendean frogatutako emaitza, hain zuzen ere.

2. ALJEBRAREN OINARRIZKO ZENBAIT EMAITZA

2.1. Polinomioak

Gogora dezagun Gaussen honako emaitza hau, *Gaussen lema* izenekoa: baldin eta $f(x) \in \mathbb{Z}[x]$ polinomio monikoa $f(x) = g(x) \cdot h(x)$ moduan deskonposatzen bada, $g(x)$, $h(x) \in \mathbb{Q}[x]$ izanik, orduan $g(x)$, $h(x) \in \mathbb{Z}[x]$ daudela ondoriozta daiteke. Bide beretik, $f(x)$ laburtezina bada $\mathbb{Z}[x]$-n, orduan $f(x)$ $\mathbb{Q}[x]$-n ere laburtezina dela ondorioztatzen da.

2.2. Kongruentziak

> **1. teorema (Dirichlet-en teorema).** Elkarrekiko lehenak diren (n, m) zenbaki osoen edozein bikoterentzat, infinitu p zenbaki lehen aurki daitezke zeinentzat $p \equiv n \pmod{m}$ baita. Emaitza horren beste bertsio baten arabera: $m \in \mathbb{N}$ emanda, existitzen dira infinitu p zenbaki lehen non $p \equiv 1 \pmod{m}$ den.

2. teorema (Hondar Txinatarren teorema). Baldin eta zkh$(m_i, m_j) = (m_i, m_j) = 1$ badira, $i \neq j$ eta $m_i \in \mathbb{N}$; eta baldin eta $a_i \in \mathbb{Z}$ badira, orduan honako ekuazio lineal hauetako sistemak,

$$x \equiv a_1 (\text{mod } m_1)$$
$$x \equiv a_2 (\text{mod } m_2)$$
$$\ldots\ldots$$
$$x \equiv a_n \, (\text{mod } m_n),$$

$m = m_1 \ldots m_n$ moduluarekiko $x \in \mathbb{Z}$ emaitza bakarra du.

3. GALOISEN TEORIA

Atal honetan, Galoisen teoriaren oinarrizko kontzeptu eta emaitza batzuk aurkeztuko ditugu. Has gaitezen egitura sinpleena gogorarazten: talde-egitura, hain zuzen ere.

3.1. Talde-egitura

G multzo batek eta $*$ haren gainean definitutako eragiketak *talde-egitura* osatzen dutela esango dugu, baldin eta G-n $*$ eragiketa elkarkorra bada, G-n $*$-rekiko elementu neutroa existitzen bada, eta G-ko elementu guztiak alderanzgarriak badira $*$-rekiko. Gainera, $*$ eragiketa trukakorra bada, taldea *abeldarra* dela esango dugu.

Talde baten *ordena*, $|G|$ idazten duguna, G multzoaren kardinala da, eta $|G| < \infty$ bada, *talde finitua* dela diogu.

Bestalde, G taldea eta H, G-ren azpimultzo ez-hutsa izanik, H G-ren *azpitaldea* dela diogu, $H \leq G$ bidez idatziko duguna, G taldeko $*$ eragiketarekin $(H, *)$ taldea denean.

Gainera, N G-ren azpitaldea bada, N G-ren *azpitalde normala* dela esango dugu, $N \trianglelefteq G$ bidez adieraziko duguna, baldin eta $n \in N$ eta $g \in G$ guztietarako, $n^g = g^{-1}ng \in N$ betetzen bada.

Taldeak sortzaile kopuru finitua onartzen duenean, *finituki sortua* dela esango dugu, eta elementu bakar batekin sor daitekeenean, *talde ziklikoa* deritzogu.

Azkenik, honako 3. teorema hau aurkeztu orduko, ekar ditzagun gogora bi taldeen arteko biderkadura kartesiarra, talde baten bi azpitaldeen barruko biderkadura zuzena, eta bi taldeen arteko kanpoko biderkadura zuzena. Badakigunez, G_1 eta G_2 edozein bi talde emanda, beren *biderkadura kartesiarra* $G_1 \times G_2$ eraiki dezakegu: elementuak (g_1, g_2) bikoteak dira, eta eragiketa osagaiz osagai egiten da. Bestalde, baldin eta G taldeak H eta N

bi azpitalde baditu, non $H \trianglelefteq G$, $N \trianglelefteq G$, $G = H\,N$ eta $H \cap N = \{1\}$ izanik, orduan G taldea H eta N azpitaldeen *barruko biderkadura zuzena* dela esaten dugu. Horrez gain, G_1 eta G_2 edozein bi talde emanda, $G_1 \times G_2$ *kanpoko biderkadura zuzena* deritzogu $G_1^* = \{(g_1, 1) \mid g_1 \in G_1\}$ eta $G_2^* = \{(1, g_2) \mid g_2 \in G_2\}$ azpitaldeen barruko biderkadura zuzenari, non azpitalde horiek G_1-en eta G_2-ren isomorfoak baitira, hurrenez hurren.

3. teorema (Talde abeldarren deskonposizio-teorema). Izan bedi G finituki sortua den talde abeldarra. Orduan, existitzen dira $r \geq 0$ osoa eta $(d_1, \ldots, d_m)$ 1 baino handiagoak diren zenbaki arrunten segida bakarra, non $d_m \mid d_{m-1} \mid \cdots \mid d_1$ baita, eta

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\,\mathbb{Z} \cong C_\infty^r \times C_{d_1} \times \cdots \times C_{d_m}$$

(× *goian aipatutako kanpoko biderkadura zuzena izanik*)

Bereziki, G talde abeldarra finitua bada, orduan $r = 0$ dugu; kasu horretan existitzen da $(d_1, \ldots, d_m)$ 1 baino handiagoak diren zenbaki arrunten segida bakarra, non $d_m \mid d_{m-1} \mid \cdots \mid d_1$ baita, eta

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z} \cong C_{d_1} \times \cdots \times C_{d_m}.$$

3.2. **Gorputzak eta hedadurak**

R multzoa eta haren gaineko bi eragiketa, + eta ·, izanik, $(R, +, \cdot)$ *identitatedun eraztun trukakorra* dela esango dugu, baldin eta $(R, +)$ talde trukakorra bada, · eragiketa elkarkorra bada, · eragiketa banakorra bada + eragiketarekiko, · trukakorra bada, eta · eragiketarekiko elementu neutroa existitzen bada.

Bestalde, baldin eta R identitatedun eraztuna bada, $x \in R$ elementua *unitatea* dela diogu alderantzizkoa badu · eragiketarekiko. Horrez gain, eraztunaren unitateen multzoak, $\mathcal{U}(R)$ bidez adieraziko dugunak, · eragiketarekiko talde-egitura du. Azkenik, $(K, +, \cdot)$ *gorputza* izango da, baldin eta K ez bada tribiala, K identitatedun eraztun trukakorra bada, eta $\mathcal{U}(K) = K - \{0\} = K^*$ badugu. Bereziki, jakina da gorputz finitu baten unitateen talde biderkakorra (· eragiketarekiko) ziklikoa dela, eta, bereziki, talde abeldarra dela.

$f : K \to L$, K eta L bi gorputzen arteko *homomorfismoa* dela esaten da, baldin eta edozein $x, y \in K$ balioetarako, $f(x + y) = f(x) + f(y)$ eta $f(x \cdot y) = f(x) \cdot f(y)$ baldintzak betetzen badira, eta $f(1_K) = 1_L$ bada. Gainera, f homomorfismoa bijektiboa bada, *isomorfismoa* dela esango dugu, haren alderantzizko aplikazioa ere homomorfismoa izanik; kasu horretan, K eta L isomorfoak direla esango dugu, $K \cong L$ adieraziz. Bestalde, multzo batetik multzo berera doan isomorfismoari *automorfismo* deritzogu.

Baldin eta K eta F bi gorputz badira, non $K \subseteq F$ den, orduan F-k eta K-k *gorputz-hedadura* osatzen dutela esango dugu, F/K bidez adieraziz.

Bestalde, F/K gorputz-hedadura baten *maila*, $[F : K]$ idatziko duguna, F-k K-espazio bektorial gisa duen K-dimentsioa da, eta maila hori finitua denean F/K (gorputz-) hedadura finitua dela diogu. Gainera, E gorputza F/K hedaduraren tarteko gorputza bada, mailaren propietate biderkakorra beteko da; hau da, $[F : K] = [F : E] \cdot [E : K]$ da.

3.3. **Galoisen hedadurak**

F/K (gorputz-) hedadura emanda, $\sigma : F \to F$, *K-automorfismoa* dela esango dugu, baldin eta σ, K-ko elementuak finko mantentzen dituen automorfismoa bada. Gainera, F/K hedadura finitua bada, F-ren K-automorfismoek konposaketa-eragiketarako osatzen duten taldea $\mathrm{Aut}_K F$ bidez adierazten da.

Edozein F/K gorputz-hedadura finiturako $| \mathrm{Aut}_K F | \leq [F : K]$ betetzen da; aurreko desberdintza berdintza denean, F/K gorputz-hedadurari *Galoisen hedadura* deritzogu, eta bere $\mathrm{Aut}_K F$ Galoisen taldea $\mathrm{Gal}_K(F)$ bidez ere adieraziko da.

F/K gorputz-hedadura eta $S \subseteq \mathrm{Aut}_K F$ izanik, S-ren *azpigorputz finkoa*, $\mathcal{F}(S)$ edo F^S bidez adieraziko duguna, $\mathcal{F}(S) = \{u \in F \mid \sigma(u) = u, \forall \sigma \in S\}$ multzoari deritzo, $K \subseteq \mathcal{F}(S) \subseteq F$ izanik.

> **4. teorema (Galoisen teoriako oinarrizko teorema).** Izan bitez F/K Galoisen hedadura, $\mathcal{A} = \{F/K$ hedaduraren tarteko gorputzak$\}$ eta $\mathcal{B} = \{\mathrm{Gal}_K(F)$-ren azpitaldeak$\}$. Defini ditzagun honako bi aplikazio hauek:
>
> $$\rho : \begin{array}{ccc} \mathcal{A} & \to & \mathcal{B} \\ E & \mapsto & \mathrm{Gal}_E(F) \end{array} \qquad \text{eta} \qquad \psi : \begin{array}{ccc} \mathcal{B} & \to & \mathcal{A} \\ H & \mapsto & \mathcal{F}(H) = F^H \end{array}$$
>
> Honako baieztapen hauek betetzen dira:
>
> (i) ρ eta ψ aplikazioak elkarrekiko alderantzizkoak dira.
>
> Beraz, bijekzio bat era daiteke F/K hedaduraren tarteko gorputzen eta $\mathrm{Gal}_K(F)$-ren azpitaldeen artean, eta horri *Galoisen korrespondentzia* deritzo.
>
> (ii) Baldin eta $E_1 \subseteq E_2$ bada, orduan, $\mathrm{Gal}_{E_2}(F) \subseteq \mathrm{Gal}_{E_1}(F)$ da, eta baldin eta $H_1 \subseteq H_2$ bada, orduan, $\mathcal{F}(H_2) \subseteq \mathcal{F}(H_1)$.
>
> (iii) Alde bateko mailak beste aldeko indizeen berdinak dira; hau da: $[E_2 : E_1] = | \mathrm{Gal}_{E_1}(F) : \mathrm{Gal}_{E_2}(F)|$ eta $|H_2 : H_1| = [\mathcal{F}(H_1) : \mathcal{F}(H_2)]$.
>
> (iv) Horrez gain, E/K Galoisen hedadura da baldin eta soilik baldin $\mathrm{Gal}_E(F) \trianglelefteq \mathrm{Gal}_K(F)$ bada. Hala izanez gero, $\mathrm{Gal}_K(E) \cong \dfrac{\mathrm{Gal}_K(F)}{\mathrm{Gal}_E(F)}$.

https://doi.org/10.1387/ekaia.22955

3.3.1. **Hedadura ziklotomikoak**

K gorputza izanik, *F*/*K* hedadura ziklotomikoa dela diogu, baldin eta *F* gorputza *K*-ren gaineko $x^m - 1$ polinomioaren deskonposizio-gorputza bada, $m \in \mathbb{N}$ baterako. Jar dezagun $\zeta = e^{2\pi i/m}$, hau da, unitatearen jatorrizko m. erroa dena. Orduan, $\mathbb{Q}$-ren gaineko hedadura ziklotomikoak $\mathbb{Q}(\zeta)/\mathbb{Q}$ motako hedadurak dira, non $\mathbb{Q}(\zeta)$ gorputza $x^m - 1$ polinomioaren deskonposizio-gorputza baita $\mathbb{Q}$-ren gainean. Gainera, $x^m - 1$ polinomioak ez du erro anizkoitzik, eta hemendik ondoriozta daiteke $\mathbb{Q}(\zeta)/\mathbb{Q}$ Galoisen hedadura dela, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(m)$ izanik, non φ Eulerren funtzioa baita. (Gogoratu Eulerren funtzioa $m \in \mathbb{N}$ balioetarako honako era honetan definitzen dela: $\varphi(m) = |\{i \in \mathbb{N}, 1 \leq i < m \mid \text{zkh}(i, m) = 1 \text{ baita}\}|$.)

Horrez gain, $m \in \mathbb{N}$ eta $\zeta \in \mathbb{C}$ unitatearen jatorrizko *m*. erroa izanik, $\mathbb{Q}$-ren gaineko *m*. *polinomio ziklotomikoa* deritzogu honako polinomio honi:

$$\Phi_m(x) = \prod_{\substack{i=1 \\ (i,m)=1}}^{m-1} \left(x - \zeta^i\right) \in \mathbb{Q}(\zeta)[x].$$

$\Phi_m(x)$ polinomioaren erroak unitatearen jatorrizko *m*. erro guztiak dira, eta denak desberdinak dira. Orain, $\Phi_m(x)$ polinomioaren maila, $\text{dg}(\Phi_m(x))$ bidez adierazten dena, $\varphi(m)$ da. Jakina da $\Phi_m(x)$ polinomioa $\mathbb{Q}$ gainean laburtezina dela, $\Phi_m(x) \in \mathbb{Z}[x]$ betetzen dela, eta $\Phi_m(x)$ polinomioaren gai askea 1 dela.

Gainera, ζ unitatearen jatorrizko edozein *m*. errorentzat, $\text{Irr}(\zeta, \mathbb{Q}) = \Phi_m(x)$ da. (Gogoratu $\text{Irr}(\zeta, \mathbb{Q})$ deritzogula $\mathbb{Q}[x]$-n koefizienteak dituen, $\mathbb{Q}[x]$-n laburtezina den, eta ζ-n anulatzen den polinomio monikoari). Ondorioz, $\mathbb{Q}(\zeta)/\mathbb{Q}$ hedaduraren maila, hau da, $[\mathbb{Q}(\zeta) : \mathbb{Q}]$, $\varphi(m)$-ren balioa du.

Bestalde, aurreko egoeretan ($m \in \mathbb{N}$ eta *K* gorputza izanik), $\mu_m(K)$ deritzogu *K* gorputzean unitatearen *m*. erroen multzoari. Orain, nabaria da honako berdintza hau:

$$\Phi_m(x) = \prod_{\substack{\zeta \in \mu_m(\mathbb{C}) \\ o(\zeta)=m}} (x - \zeta). \tag{1}$$

Azkenik, $m \in \mathbb{N}$ zenbaki arruntetarako $\Psi_m(x)$ idazkeraren bidez adieraziko dugu honako polinomio hau:

$$\Psi_m(x) = \prod_{\substack{\zeta \in \mu_m(\mathbb{C}) \\ o(\zeta)\neq m}} (x - \zeta). \tag{2}$$

Ohartu $\Phi_m(x)\Psi_m(x) = x^m - 1$ dela.

5. teorema. Baldin eta $m \in \mathbb{N}$ bada, taldeen arteko honako isomorfismo hau dugu:

$$\psi : \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m)) \to \mathcal{U}(\mathbb{Z}/m\mathbb{Z}), \qquad \zeta_m = e^{2\pi i/m} \text{ izanik.}$$

Orain, **2.2** atalean aurkeztutako 1. teorema (Dirichlet-en Teorema) frogatuko dugu. (Ikusi [4].)

1. teoremako enuntziatua. Izan bedi $m \in \mathbb{N}$. Orduan, existitzen dira infinitu p zenbaki lehen, non $p \equiv 1 \pmod{m}$ den.

Froga. $m = 1$ kasurako emaitza tribiala da; beraz, har dezagun $m > 1$. Absurdura eramanez, suposa dezagun p zenbaki lehen kopuru finitua dagoela non $p \equiv 1 \pmod{m}$ den. Izan bedi S zenbaki lehen horien multzoa, eta defini dezagun $P = \prod_{p \in S} p$.

Nabaria da $\Phi_m(x) \pm 1$ polinomioaren erroen kopurua finitua dela. Beraz, har dezagun k zenbaki osoa, zeinentzat $\Phi_m(kmP) \neq \pm 1$, eta zeinentzat existitzen baita p_0 zenbaki lehen bat ere $\Phi_m(kmP)$ zatitzen duena. Ondorioz, $\mathbb{F}_{p_0}[x]$ eraztunean lan eginda, $\overline{\Phi_m}(\overline{kmP}) = \overline{0} \in \mathbb{F}_{p_0}$ dugu; hau da, $\overline{kmP}$, $\overline{\Phi_m}$-ren erroa da.

Bestalde, hedadura ziklotomikoko atalaren azken paragrafoetako (1) eta (2) ekuazioetatik, $\mu_m(\mathbb{C})$, $x^m - 1 \in \mathbb{Z}[x]$ polinomioaren erro konplexuen multzoa izanik, $\Phi_m(x) \cdot \Psi_m(x) = x^m - 1$ erlazioa nabari betetzen da, eta, bereziki, honako hau dugu:

$$\Phi_m(kmP) \cdot \Psi_m(kmP) = (kmP)^m - 1.$$

Egoera honetan, $p_0 \nmid m$ ondorioztatzen da. Horrez gain, $\Phi_m(kmP)$ polinomio gisa interpretatuz, bere gai askea 1-en berdina da. Beraz, emaitza horretatik, eta $\overline{\Phi_m}(\overline{kmP}) = \overline{0} \in \mathbb{F}_{p_0}$ denaren emaitzatik, $p_0 \nmid kmP$ ondorioztatzen da. Bereziki, $p_0 \nmid P$ eta $p_0 \notin S$.

Adieraz dezagun $x^m - 1$ polinomioa $f(x)$ bidez, eta $\overline{f} = \overline{1}x^m - \overline{1} \in \mathbb{F}_{p_0}[x]$. Orduan, $\overline{f}' = \overline{m}x^{m-1} \in \mathbb{F}_{p_0}[x]$ polinomioa ez nulua da, $p_0 \nmid m$ delako.

Ondoren, ohar gaitezen $\overline{f}$ polinomioak ez duela erro anizkoitzik. Izan ere, baldin eta α $\overline{f}$-ren erro anizkoitza balitz, $\overline{1}\alpha^{m-1} = \overline{0} \in \mathbb{F}_{p_0}$ litzateke, eta, ondorioz, aldi berean, $\alpha^m = \alpha^{m-1}\,\alpha = \overline{0} \in \mathbb{F}_{p_0}$, eta $\alpha^m = \overline{1}$ beteko lirateke; horiek bata bestearen kontrakoak dira, $\overline{0} \neq \overline{1}$ delako.

Berriro ere, $\Phi_m(x) \cdot \Psi_m(x) = x^m - 1 = f(x)$ erlazioa erabiliz, $\mathbb{F}_{p_0}$ eraztunera pasatuz, honako hau dugu:

$$\overline{\Phi_m}(x)\cdot\overline{\Psi}(x)=\overline{1}x^m-\overline{1}=\overline{f}.$$

Orain $\overline{kmP}$ elementua $\overline{\Phi}_m(x)$-ren erroa denez, ezin daiteke $\overline{\Psi}_m(x)$-ren erroa izan. Hortaz, $\overline{kmP}$, $\mathbb{F}^*_{p_0}$-ren unitatearen jatorrizko m. erroa da.

Beraz, Lagrangeren teoremagatik, $m=|\langle\overline{kmP}\rangle|$ zenbakiak $|\mathbb{F}^*_{p_0}|=p_0-1$ zatitzen duela ondorioztatzen da. Ondorioz, $p_0\equiv 1 \pmod m$ lortzen da, eta, oraingoan, $p_0\in S$ dugula ondorioztatzen da. Azkenik, lortutako emaitza argudioan garatutako emaitza baten kontrakoa denez, horrek esan nahi du infinitu p zenbaki lehen daudela, non $p\equiv 1 \pmod m$ den. □

4. **KRONECKER-WEBERREN TEOREMA**

6. teorema (Kronecker-Weberren teorema). Edozein A talde abeldar finitu $F/\mathbb{Q}$ Galoisen hedaduraren baten $\mathrm{Gal}_{\mathbb{Q}}(F)$ Galoisen taldearen isomorfoa da.

Froga. Izan bedi A talde abeldar finitua. Orduan, talde abeldarren deskonposizio-teoremagatik (3. teorema), badakigu existitzen dela $(d_1,\ldots,d_m)$ 1 baino handiagoak diren zenbaki arrunten $(d_1,\ldots,d_m)$ segida bakarra, non $d_m\mid d_{m-1}\mid\cdots\mid d_1$ baita, eta

$$A\cong C_{d_1}\times\cdots\times C_{d_m}.$$

Aukera ditzagun p_i zenbaki lehen desberdinak, zeinentzat $p_i\equiv 1 \pmod{d_i}$. Aipatutako zenbaki lehen desberdinen existentzia ziurtatuta dago 1. teoremagatik. Orain, defini ditzagun honako aplikazio hauek:

$$\phi_i:(\mathbb{Z}/(p_i-1)\mathbb{Z},+)\cong C_{p_i-1}\ \to\ (\mathbb{Z}/d_i\mathbb{Z},+)\cong C_{d_i}$$

$$\overline{a}=a+(p_i-1)\mathbb{Z}\ \mapsto\ \overline{\overline{a}}=a+d_i\mathbb{Z}.$$

Erraz ikus daiteke aplikazioa hauek homomorfismo supraiektiboak direla. Izan ere, edozein $\overline{a},\overline{b}\in\mathbb{Z}/(p_i-1)\mathbb{Z}$-rako $\phi_i(\overline{a}+\overline{b})=\phi_i(\overline{a+b})=\overline{\overline{a+b}}=\overline{\overline{a}}+\overline{\overline{b}}=\phi_i(\overline{a})+\phi_i(\overline{b})$. Bestetik, edozein $\overline{\overline{c}}\in\mathbb{Z}/d_i\mathbb{Z}$-rako nahikoa da $\overline{c}\in\mathbb{Z}/(p_i-1)\mathbb{Z}$ aukeratzea, zeinentzat $\phi_i(\overline{c})=\overline{\overline{c}}$ baita, $p_i-1\equiv 0 \pmod{d_i}$ baldintzak betetzen direlako.

Orain, ezkerreko eta eskuineko taldeen arteko kanpoko biderkadura zuzena eginez, $\prod_{i=1}^m\mathbb{Z}/(p_i-1)\mathbb{Z}$ taldetik, $\prod_{i=1}^m\mathbb{Z}/d_i\mathbb{Z}\cong\prod_{i=1}^m C_{d_i}\cong A$ taldera ϕ deituriko homomorfismo supraiektibo naturala eraiki daiteke.

Bestalde, jakina dugu edozein $\mathbb{Z}/p\mathbb{Z}$ gorputz finitu baten unitateen talde biderkakorra $p-1$ ordenako talde ziklikoa dela; hau da, $(\mathcal{U}(\mathbb{Z}/p\mathbb{Z}),\cdot)\cong C_{p-1}\cong(\mathbb{Z}/(p-1)\mathbb{Z},+)$.

Adieraz dezagun $n = p_1 \ldots p_m$, non edozein $1 \leq i, j \leq m$ desberdinetarako $(p_i, p_j) = 1$ baita, p_i zenbaki lehenak desberdinak direlako. Egoera horietan, Hondar Txinatarren teoremagatik existitzen da egoki aukeratutako kongruentzia-sistema baten emaitza bakarra n moduluarekiko, zeinekiko $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ eta $\mathcal{U}(\mathbb{Z}/p_1\mathbb{Z}) \times \cdots \times \mathcal{U}(\mathbb{Z}/p_m\mathbb{Z})$ taldeen artean homomorfismo bijektibo bat eraiki daitekeen.

Orain, arinago aipatutako homomorfismoak egoki konbinatuz eta konposatuz: lehenbizi, $\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \cong \mathcal{U}(\mathbb{Z}/p_1\mathbb{Z}) \times \cdots \times \mathcal{U}(\mathbb{Z}/p_m\mathbb{Z})$ taldetik $\prod_{i=1}^{m} \mathbb{Z}/(p_i - 1)\mathbb{Z}$ taldera, eta, ondoren, $\prod_{i=1}^{m} \mathbb{Z}/(p_i - 1)\mathbb{Z}$ taldetik $\prod_{i=1}^{m} \mathbb{Z}/d_i\mathbb{Z} \cong \prod_{i=1}^{m} C_{d_i} \cong A$ taldera; orduan, $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ taldetik A taldera honako diagrama honetan agertzen den Φ homomorfismo supraiektiboa eraiki daiteke.

$$\begin{array}{ccc}
A & \longleftarrow & C_{d_1} \times \ldots \times C_{d_m} \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_m\mathbb{Z} \\
\Big\uparrow\!\!\Big\uparrow & & \Big\uparrow\!\!\Big\uparrow \phi \\
\Phi & & C_{p_1-1} \times \ldots \times C_{p_m-1} \cong \mathbb{Z}/(p_1-1)\mathbb{Z} \times \ldots \times \mathbb{Z}/(p_m-1)\mathbb{Z} \\
\Big\uparrow & & \Big\updownarrow \\
\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) & \longleftarrow & \mathcal{U}(\mathbb{Z}/p_1\mathbb{Z}) \times \cdots \times \mathcal{U}(\mathbb{Z}/p_m\mathbb{Z})
\end{array}$$

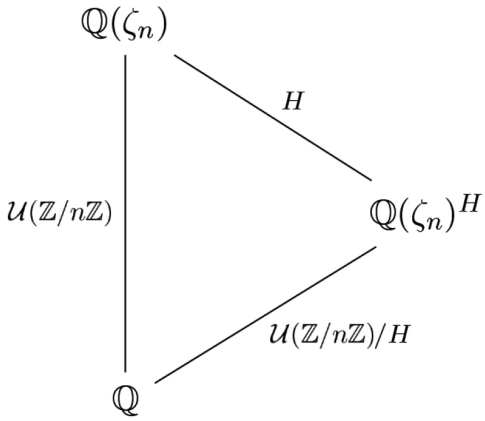
Adieraz dezagun $\mathrm{Ker}\Phi = H$ bidez. Bereziki, $H \trianglelefteq \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ da. Orduan, isomorfiazko lehenengo teoremagatik, badakigu $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})/H \cong A$ dela. Beraz, Galoisen hedadura, zeinaren bere Galoisen taldea eta $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})/H$ taldea isomorfoak baitira, aurkitzea baino ez zaigu falta.

Bestalde, badakigu 5. teoremagatik, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, Galoisen hedaduraren Galoisen taldea $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ taldearen isomorfoa dela, $\zeta_n = \zeta = e^{2\pi\imath/n}$ izanik. Orain, Galoisen teoriako oinarrizko teoremagatik (4. teorema), $H \leq \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ azpitaldeari $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ hedadurako $\mathcal{F}(H) = \mathbb{Q}(\zeta_n)^H$ azpigorputz finkoa dagokio, zeinentzat $\mathrm{Gal}_{\mathcal{F}(H)}(\mathbb{Q}(\zeta_n)) = \mathrm{Gal}_{\mathbb{Q}(\zeta_n)^H}(\mathbb{Q}(\zeta_n)) = H$ baita.

Horrez gain, $H \trianglelefteq \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ denez, 4. teoremako (iv) atalagatik, aurkitutako $\mathbb{Q}(\zeta_n)^H/\mathbb{Q}$ gorputz-hedadura Galoisen hedadura dela ondorioztatzen da, bere Galoisen taldea

$$\mathrm{Gal}_{\mathbb{Q}}\left(\mathbb{Q}\left(\zeta_n\right)^H\right) \cong \frac{\mathrm{Gal}_{\mathbb{Q}}\left(\mathbb{Q}\left(\zeta_n\right)\right)}{\mathrm{Gal}_{\mathbb{Q}(\zeta_n)^H}\left(\mathbb{Q}\left(\zeta_n\right)\right)} \cong \frac{\mathcal{U}\left(\mathbb{Z}/n\mathbb{Z}\right)}{H} \cong A \quad \text{izanik.}$$

Frogaren azken zatia honako diagrama honen bitartez irudika daiteke, lerroen goiko muturretan $\mathbb{Q}$ gaineko aipatutako Galoisen hedadurak adieraziz, eta lerroen artean haiei dagozkien Galoisen taldeak.



BIBLIOGRAFIA

[1] RUIZA M., FERNÁNDEZ T. eta TAMARO E. 2004. «Biografía de Évariste Galois. Biografías y Vidas». *La enciclopedia biográfica en línea*.

[2] HAROLD M. EDWARDS. 1984. *Galois Theory*. Springer Graduate Texts in Mathematics.

[3] TIESINGA H.G.J., TOP J. eta STERK A.E. 2016. «The inverse Galois problem: Bachelor Project Mathematics». *Faculty of Mathematics and Natural Sciences, University of Groningen*.

[4] DEAN YATES. 2017. «The Inverse Galois Problem: 4th year project». *Queen Mary, University of London*.

[5] NÚRIA VILA. 1992. «On the Inverse Problem of Galois Theory». *Publicacions Matemátiques*, **36**, 1053-1073.

[6] FRANS KEUNE. 2015. *Galoistheorie*. Epsilon Uitgaven, Nederlands.

[7] VAN DER WAERDEN B. L. 1930. *Modern Algebra*. Springer-Verlag, Germany.